SENIOR SERVICE COLLEGE FELLOWSHIP RESEARCH PAPER

ARMY INFORMATION TECHNOLOGY STRATEGIC PLANNING AND PROCUREMENT PROCESS

BY

LIEUTENANT COLONEL KATHLEEN SWACINA
United States Army Reserve

USAWC CLASS OF 2002
Senior Service Fellow

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013

USAWC FELLOWSHIP RESEARCH PROJECT

ARMY INFORMATION TECHNOLOGY STRATEGIC PLANNING AND PROCUREMENT PROCESS

by

LIEUTENANT COLONEL KATHLEEN SWACINA
United States Army Reserve

Dr. Jerry Davis
Project Advisor
The University of Texas at Austin

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Lieutenant Colonel Kathleen Swacina

TITLE: Army Information Technology Strategic Planning and Procurement Process

FORMAT: Fellowship Research Project

DATE: 09 April 2002 PAGES: 52 CLASSIFICATION: Unclassified

The purpose of this research is to provide a better understanding of how the Army's Information Management (IM) Plan should link with the *Quadrennial Defense Review (QDR)*, the *Joint Vision 2010 (JV2010)*, and the *Department of Defense (DoD) Information Management Plan* already in existence. Each DoD Information Technology (IT) goal is examined and planning techniques are suggested to fulfill the objectives. Next to personnel and training, resourcing for IT is the most costly investment the Army makes. In the past, the lack of a cohesive IT Operations Plan has made budgeting for the existing and newly proposed systems haphazard at best. With the increased concern in Homeland Defense, it is imperative now more than ever that the Army have a defined plan of how information systems will support the core business processes, be designed and procured in a timely manner, provide rapid information, and be safeguarded against intrusion.

There is an increased call on technology to maximize the Army forces. Only by coordinating, planning, and budgeting in a timely manner can the Army hope to accomplish its ever-changing missions in both National and Homeland Defense. There must be a shift in the past methodology of systems design and procurement. As the Army moves into the new century, developing a timely and cohesive strategy for information systems fielding, security, and replacement is as important as that of any other weapon system. A well-defined IT Operations Plan is more critical than ever.

This paper is meant to be an example for the Army and its subordinate organizations to enable them to create a successful IM Strategic Plan to link their missions with the higher headquarters' goals and objectives. The goals and objectives are from the DoD IM Strategic Plan. The follow-on assessments and suggestions are those of the author and various sources as indicated. The target audience for this paper is the Chief Information Officers (CIOs) and decision-makers who have a thorough understanding of how information technology is procured and deployed.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

ARMY INFORMATION TECHNOLOGY STRATEGIC PLANNING AND PROCUREMENT PROCESS

"The next war will not be fought with guns, but with computers in offices."
Sherwood Boehlert, Republican Representative from New York

"The role information technology will play is a considerable one."
Tom Ridge, Director of the Office of Homeland Defense

Next to Personnel and Training, resource allocation for Information Technology (IT) is the Army's most costly investment. Due to the lack of a cohesive Army IT Operations Plan, budgeting for the existing and newly proposed systems has been haphazard at best. Due to the increased emphasis on Transformation and concern for Homeland Defense, it is imperative that defined planning be conducted on how information systems will support the core business processes, be designed and procured rapidly, provide timely information, and be safeguarded against intrusion. This paper will provide readers with a high level look at the Department of Defense (DoD) Information Management (IM) Strategic Plan and suggest Army solutions to the goals and objectives outlined therein.

Integration of the three Army components is necessary for success in realizing the DoD strategic vision for IM. For many years, the three components of the Army have acted as separate entities. The Active Army, National Guard, and Army Reserve all have interdependent requirements and missions, but they often do not coordinate their efforts in designing and procuring IT systems. In the past, the Army's practice in developing and fielding systems has been more of a knee-jerk, and a chain reaction of events attempting to simulate a "phased-in" approach to fielding. Often the Active Army designs and develops a system for an immediate mission need only to have the National Guard and Army Reserve scramble to modify the system to their particular mission requirements. This practice has perpetuated the stovepipe systems that currently hamper the entire Army. Most often this fielding is further impacted by

funding requests that are not compatible with the Program Objective Memorandum (POM) cycle and end up being supported by end of year funds.

A shift from the past methodology of IT systems design and procurement is imperative. Starting with the initial planning of a new system, the Army Reserve and National Guard must be present to represent and promote their specific component requirements. Funding requirements from all three Army components should be packaged together for the POM. Fielding plans must be well thought out to ensure that designated "round-out" units from the Guard and Reserve are provided the necessary systems to support the total Army mission. IT systems life-cycles should be standardized to better plan for the replacement of out-dated systems and incorporate the newest technology possible. This will provide better information operations security over all. As the Army moves into the new century, developing a timely and cohesive strategy for information systems fielding, security, and replacement is as important as that of any other weapon system.

In planning for accomplishment of any objective, the starting point should be an established vision. The vision for information technology as stated in the DoD IM Strategic Plan, dated October 1999, is as follows:

> Information superiority achieved through global, affordable, and timely access to reliable and accurate information for worldwide decision making and operations.[1]

A well-defined Information Technology Operations Plan is the first critical step in realizing the vision. There is an increased call for technology to maximize lethality, mobility, and information superiority of the Army's resources. Only by properly coordinating, planning, and budgeting in a timely manner, can the Army hope to achieve its ever-expanding mission in National and Homeland Defense.

But how does the Army get there? Each (Army) component has a different operational design based on its individual need and uses of the information. Although the same data elements

may be used in all the Army components, these elements are packaged differently. The Army components must integrate their IT efforts to succeed in achieving the DoD Strategic Vision. To accomplish this vision, DoD has established the IT strategic mission statement and four major supporting goals. These are described as follows:

> MISSION: Provide, in a secure fashion, the right information, at the right place and time from the right sources, in a form that users can understand and reliably use to accomplish their missions and tasks, effectively and efficiently.
>
> Goal 1 - Become a Mission Partner – the integrating of IM with our national defense mission using joint mission planning and analysis processes as the basis for defining information service and performance requirements.
>
> Goal 2 – Provide Services that Satisfy Customer Information Needs - responds to management direction and mission requirements by delivering quality, affordable products and services to IM/IT customers.
>
> Goal 3 – Reform IT Management Processes to Increase Efficiency and Mission Contribution - emphasizes management process improvements that are needed to more effectively deliver information and services to DoD mission customers.
>
> Goal 4 – Ensure the DoD's Vital Information Resources are Secure and Protected - reflects the pervasive impact of information assurance on DoD. The strategies associated with the goals are organized logically but are intended to be implemented in parallel to make rapid progress toward the goals.[2]

DoD has linked objectives and strategies to achieve these goals. They are organized in such a way as to imply that they be worked in parallel for rapid goal achievement. Figure 1 shows the goals and supporting objectives in this parallel relationship.

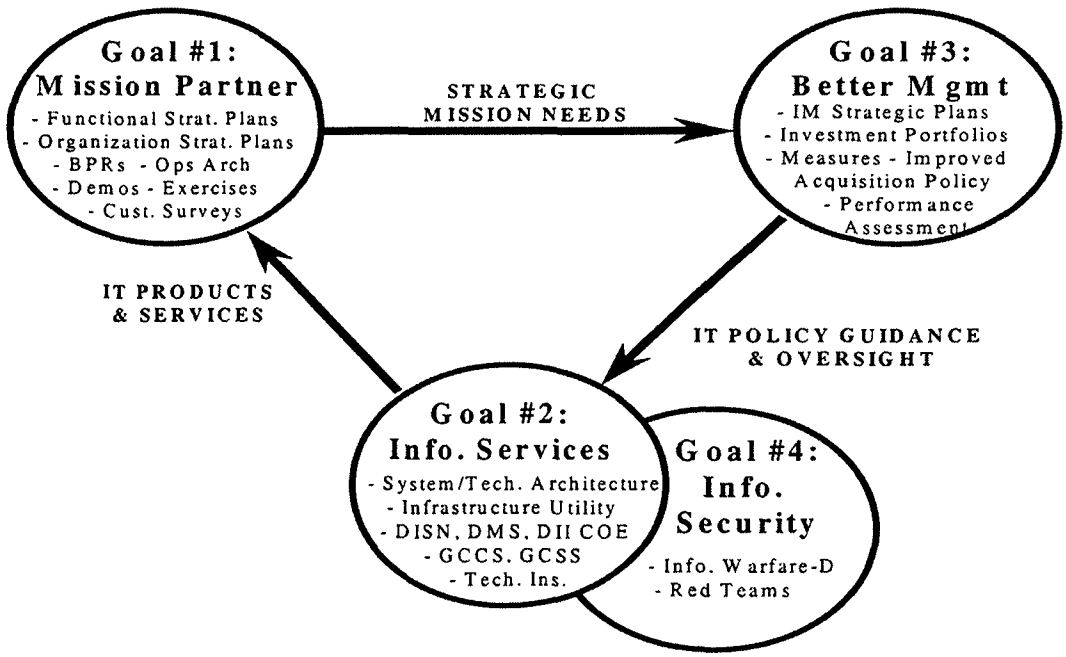

FIGURE 1. KEY RELATIONSHIPS BETWEEN THE IM GOALS

The DoD IT vision, mission, and goals were all developed well before the September 11, 2001 terrorist attacks. Therefore, DoD and the Army must decide how the requirements for the Information Management Plan will change. How will development of the Homeland Defense Office influence this plan? How will the Transformation of DoD and the Army higher headquarters impact on the current plan? These are questions the Army Chief Information Officer (CIO/G-6) is currently addressing.

The recent change to the *Quadrennial Defense Review (QDR)* will also drive changes to the DoD IM Plan. In a fast changing world, strategic planning can no longer remain a linear process that attempts to work in all situations. In the Cold War, strategic plans were designed to be vague and flexible enough to theoretically work in any situation. Drs. Rea and Kerzner state in their book *Strategic Planning a Practical Guide*:

> Traditionally strategic planning has not led to a single school of thought on a set of concepts that work well in all circumstances. Chandler in 1962 said, "if we formulate long-term goals and marshal the resources at hand around those goals, then we can create a 'vision of success' as Mintzberg called it so that free will and intentional design, according to Porter, can be applied to the strategy." [3]

If each DoD goal is examined, and capability-based planning techniques are applied, as opposed to the traditional threat-based planning practiced since the 1980s, then a cohesiveness to the fragmented process of IT strategic planning can be achieved. At the initiation of the planning process resources can be programmed and directed to support each goal.

The remainder of this paper will address DoD goals and objectives, and provides suggestions and examples of programs, to support the Army in fulfilling the DoD plan. The goals and objectives as listed are direct quotes from the DoD Information Management Plan. The follow-on assessments and suggestions are the author's, based on personal experience and supported by a variety of sources as indicated.

GOALS, OBJECTIVES, AND STRATEGIES

GOAL 1. BECOME A MISSION PARTNER.

General Kern, Commanding General for the Army Material Command (AMC), stated that systems must be integrated into "systems of systems." This means collaboration among the Army commands, Defense Advanced Research Projects Agency, industry and academia must be achieved to realize a successful Army Transformation. The *Joint Vision Plan (JV2010)* implies that in the future information will be as important on the battlefield as any weapon system. By partnering with DoD, as well as with private industry, the Army can multiply its resources for mission capability. The DoD IM Plan states:

> *JV2010* recognizes information superiority as the enabler for full spectrum dominance in the 21st century.[4]

The *QDR* calls for a comprehensive review of military strategy and the modernization of the DoD-wide approach to business information. This translates to the pushing down of information to the lowest level possible to enable decision-making at the correct action level. This will enable the vision of flattening and/or streamlining the Army to take advantage of the rapid flow of data and information. In this way technology is able to greatly enhance the capabilities of mission performance.

The first objective to support goal 1 is to "identify mission needs and align IT." IT personnel must be on the team at the beginning of organizational strategic planning. As mission requirements are identified IT can be designed to support these needs. There are basically three strategy alternatives as outlined in *Breakthrough Technology Project Management* by Lientz and Real:

> First is no strategy at all. Second is to develop and select probable scenarios and develop the technology to support the solution base for each of the scenarios and then fund each project separately. Finally to develop likely scenarios, analyze the probabilities and risks of each occurring, and then develop a collective IT strategy with enough flexibility to address the various missions.[5]

To achieve integrated IT planning and support, all organizational levels must be able to understand and clearly communicate requirements. Only with full understanding of the mission can there be linkage between operational strategy, goals, and objectives. Understanding of mission is critical in the development of the measures and overarching IT architecture that supports and enables commanders to accomplish that mission.

To date the Army has practiced the second strategy, or threat-based strategy, identified above. The policy has been to develop partial requirements for IT on the pretense of being flexible. This policy has perpetrated "project creep" due to ever-changing requirements. As new leaders take on command responsibilities, the strategy changes. The new leaders champion their perception of the mission requirements and plan accordingly. However, available funding was based on past requirements. As new strategies are developed, new

technologies must bridge the gap between the old and new requirements. Many technical projects fail due to reactive strategic planning and failure to align with the changing mission.

Applying capability-based planning can provide the flexibility to plan and fund technology for better addressing mission changes. By analyzing various scenarios and applying current technology in more imaginative ways; it is found that capability planning will provide the gap coverage to develop and field future technological needs. To be successful in seamless IT strategic planning, the Army must bridge the gap between present technology and future technological developments. In this way technological opportunities can enhance the Army's mission and strengths.

Another tool in gathering and analyzing IT requirements is the use of various parts of the architecture. Architecture consists of three parts: operational, technical, and systems. These parts are defined as follows:

- Operational architecture is a description of the tasks and activities, operational elements, and information flows required in accomplishing or supporting a military operation.
- Technical architecture is the minimal set of rules governing the arrangement, interaction, and interdependence of the parts or elements whose purpose is to ensure that a conformant system satisfies a specific set of requirements.
- Systems architecture is a description, including graphics, of the systems and interconnections providing for or supporting, warfighting functions.[6]

A complete Army architecture will link the *Joint Vision 2010*, the *QDR*, the Joint Warfighting Capabilities Assessment (JWCA) process, as well as other planning and assessment capabilities into one cohesive product. A common architecture process must be approved and adopted by all Army components. This strategy envisions an assessment and analysis process that addresses all elements of military capability holistically including a Joint and Defense-wide perspective leading to supported objectives, measures, architectures, and strategies that leverage IT.

The CIO/G-6 has established a comprehensive Army Enterprise Architecture (AEA) guide for creating an integrated architecture framework for operational, systems, and technical

architectures. The Army how-to guide for defining architecture is The Army Enterprise Architecture Guidance Document (AEAGD). This guide not only addresses the development of architecture designs, but also architectural management, uses of architectures and architecture products.[7]

It only makes sense that with the ever-shrinking resource base for the Army that efforts in like processes within Army components be combined. Back office support systems and processes are logically the first to be coordinated not only across Army components, but also across the Services. The issue here is not when, but how, to ensure the Army is fully represented in these efforts.

Due to the shrinking resources the Army must take advantage of partnering with the integrated,

> Joint and Defense-wide process for assessing options and programs, and bringing new capabilities to the field. The DoD CIO Council maintains a Defense-wide plan for IT participation in exercises, demos, advanced concept technology demonstrations (ACTDs), advanced warfighting experiments (AWEs), and other front-end processes and assessment activities. Information gathering is the key during this portion of the strategy.[8]

Emerging operations concepts can result in doctrine and tactical issues. There is insufficient data concerning information requirements regarding future needs to support a structured view of the system. Modeling and simulation exercises can demonstrate how a new system will fit into the architecture. In any modeling and simulation exercise, performance measures need to be established especially in the areas of cost, capability, and reliability.

The second objective for Goal 1 is to "forge effective partnership relationships with customers." Before effective partnerships can be made, the current systems and processes need to be defined. An accurate organizational structure at all levels needs to be documented. Process ownership also needs to be established.

Ultimate responsibility for managing processes, IT investing, and assessment of IT effectiveness rests with leaders, process owners and line managers. Effective partnering requires positioning IT to influence key functional decisions. Designing organizational structures to ensure functional and IM responsibilities are effectively executed and aligned at all levels can enhance partnering. Existing management structures need to be assessed in line with the Government Paper Reduction Act (GPRA), Chief Financial Officer (CFO), and the Clinger Cohen Act (CCA) mandates. A comprehensive, top-level review of Army IT management structures by the CIO must be conducted to ensure efficient partnering at all levels of the Army and customers can be met. [9]

Drs. Rea and Kerzner in their book *Strategic Planning a Practical Guide*, make the following point on the customer being able to communicate IM strategic needs.

> "The degree to which either consumers or executives who set organizational strategy can assume rationality should be considered."[10]

"Customer" can be defined as an Army organization, a functional office, a soldier, or an outside organization. Only by educating the lower level customer on the IM mission for the higher levels in an organization can there be a common understanding of missions. Effective communication must be in the user's language, not in technical jargon. Armed with this knowledge, informed decisions can be made on what IT is needed and how to structure the architecture to be more responsive for all. "This strategy requires increased emphasis on educating users about IM's potential for improving mission performance, how to effectively work with the IM community, and how to get the most from IT investments."[11]

Gathering customer feedback at all levels is essential in customer communication. In *Best Practices Building Your Business with Customer-Focused Solutions* the authors state:

> However sophisticated the technology, the best practices in providing customer service ultimately come down to the people behind the machine – the managers who deal with customer problems in the abstract and the front-line representatives who deal with them daily on a face-to-face basis. Getting these two groups

> together – and giving them a chance to work cooperatively – is the essence of this strategy.[12]

Acting on the feedback is even more crucial to forging effective partnerships. Communication channels need to flow between the CIO, the Commanders in Chief (CINCS), and the other service and agency heads to be able to rapidly respond to needs and concerns. Customer feedback is a key influencer on strategic planning, Business Process Reengineering (BPR), and day-to-day service or information delivery.[13]

The third objective for DoD's first goal is to "move toward an information marketplace." The goal implied here is to provide "information anywhere, any time." If data can be captured that the organization uses and needs, then the data distribution can be institutionalized for use throughout the organization. By creating a knowledge-based management architecture, the Army can optimize the effectiveness of strategic and tactical decisions. The target is an agile, responsive, learning organization in which knowledge needed to provide critical mission support is available where and when needed.[14]

Data is the basis for effective and efficient business performance. Quality information is data that satisfies not only the immediate customers, but also satisfies the customers downstream without major manipulation or duplication of the data. If information is a product and knowledge workers are customers, then providing quality information means providing customer service to those knowledge workers. Knowledge workers require quality information to do their jobs. Information customer service requires defining data across the business value chain to support all knowledge workers rather than from a vertical stovepipe or organizational perspective.[15] The most effective way to provide quality information is through the increased use of performance contracts, partnering agreements, fee-for-service, and devolution of purchasing of IT to lowest levels.

All data is valuable and, depending on how it is combined, can give little or much valuable information. The issue is to be able to safeguard all the information, and allow only those personnel who have a need, to access the information. This will require a secure infrastructure. The Army has already developed the Army Knowledge On-Line (AKO) website. No Army sub-organization should create a separate website. Keeping the Army information behind a secure firewall will reduce the chances of valuable information being accessed by unauthorized individuals.

GOAL 2. PROVIDE SERVICES THAT SATISFY CUSTOMER INFORMATION NEEDS.

The difference between information and knowledge needs to be differentiated here. In an article by Yogesh Malhotra, he defines information and knowledge respectively as follows:

> Information resides on computers and has a performance link with it. Even our current architecture provides information flow both internally and externally as well as up and down the organization. However this flow of information cannot in itself create knowledge. Knowledge is distinguished with a potential for action. Knowledge resides in the customer and not in the collection of information. It is how the customer uses the information that matters.[16]

The first objective to the second DoD IT goal is to "build an infrastructure based on architectures and performance." Knowledge creation needs to start with gathering the customer requirements necessary for mission accomplishment. Surveys and analysis of most frequently asked questions or scenarios are methods for gathering these mission requirements. Having the information available on a secure, standardized grid will help facilitate the data accessibility. Therefore, a shared data environment to ensure semantic interoperability and cross-functional integration is a priority. Army organizations must move from a "technology centric" paradigm to an interconnected set of services/products with quantifiable cost and performance measures to determine the value added to the mission. The cost of the infrastructure must be reduced relative to its contribution to the mission.

The Army Transformation will have to extend to the information infrastructure. End-to-end management of the infrastructure must support the goals of seamless integration. Stovepipe systems are often narrowly focused, not fully interoperable, and support a single function or organization. Users are required to assemble information from incompatible sources. This can cause false knowledge due to conflicting information from non-verified sources. "Breaking out of this stovepipe environment requires new management mechanisms that crosscut organizational boundaries. Common and shared solutions will reduce unnecessary duplication and cut costs for everyone."[17]

Performance measures need to be established for all products and services that are to be delivered or inserted into the Army infrastructure. This will save money in the long run because vendors will be paid on a performance-based contract rather than the cash flow system presently in use. Therefore, efficiency and investment decisions can be based on systematic assessments of information cost and value added to mission customers. In their book, Mr. Peterson and Ms. Carco stated:

> Performance measures should reinforce a group perspective. The performance they measure should be weighed pragmatically.[18]

The original DoD Objective 2.2, "Ensure DoD Systems meet the Year 2000 (Y2K) Challenge," and the appropriate compliance checks, have been successfully completed for the Army. Documentation of the process used to accomplish this project is archived for future reference. An inventory of the various systems was also gathered for the Y2K Project and provided the beginnings of the Army architecture documentation.

The third objective of Goal 2, "modernize and integrate the defense information infrastructure, evolving it to the Global Information Grid (GIG)," begins with improving the base infrastructure the Army is currently operating on. Current efforts are underway to standardize the Army's base level communications, computing infrastructure, and data storage environment.

Examples of the forward momentum in systems improvements are: the Army's Network Communications (Netcom); and the Integrated Total Army Personnel Database (ITAPDB) meant to streamline and standardize the Army personnel systems. Other Army component projects such as the Reserve Component Automation Systems (RCAS), first designed to standardize the technological base for the Army, the recent data center consolidation, and the records imaging system improvements are examples of data storage improvements.

Stovepipe systems still plague the Army. Only by benchmarking, reengineering, and creating systems of systems can the Army eliminate duplication and streamline the organization.

> The Global Information Grid (GIG) policies, plans and programs will embody the constructs that will create the computing model shift to information centric operations/warfare. GIG provides the means to structure the future of the Command's computing resources to achieve the reality of information superiority. At the core of GIG is the recognition of the pervasiveness and durability of distributed computing across The Army. A networked mid-tier architecture will define the core of the GIG with the tenets of enterprise management, economies of scale, and information assurance governing its evolution.[19]

In order to realize a GIG, the Army must create a shared data environment. Shared data resources hold the information for one or more applications. Shared data resources perform two functions: information storage and information management. Storage management determines the physical location of data on the storage medium and the control of the actual data movement. Information management determines how the information is to be stored and retrieved. Data stewards, who are well versed in the business processes, need to be appointed to logically order the mission critical data items. The shared data repositories will be accessed through AKO. Decisions still need to be made as to where the data will actually reside. Through the use of virtual databases, data can be maintained close to the original source of the data and accessed as needed. The migration toward network centricity is imperative to make data available to anyone who needs it across the enterprise.

To create the GIG, standards must be set throughout the services. By using set standards the amount of diversity on the network can be minimized. DoD has provided documentation on the standardization for architecture. However, if the services are expected to combine systems and process into a seamless response force for future conflicts, then there needs to be cross communication between them. Technical interfaces can be done with relatively little effort. Human interface and understanding of the various processes is more complex. Assigning data stewards, who are the authority for the data elements' validity and the business processes, is a must for enhanced communications.

One of the major inadequacies of current IT systems is the incompatibility of communication across functional and locational boundaries. In order to digitize the Army, a number of technological improvements are needed.

> Tactical communications must be digitized and capable of transferring multi-media information such as maps and images to customers. Networks must be seamlessly integrated and managed across all levels (e.g., national, theater, tactical), and interfaces established with allies, coalition partners, and other government agencies.[20]

Interoperability of communications will enhance flexibility and will enable the Army to deploy its forces more rapidly and effectively.

DoD has outlined a strategy to move to an information dissemination management (IDM) concept. This is a drive toward the services to be knowledge management organizations. The advantage of knowledge management is that it improves awareness, access, and delivery of information across the full spectrum of operations. The AKO portal with its hypertext links is the backbone for the Army knowledge dissemination effort. Using commercial-off-the-shelf (COTS) products for future improvements will increase the capabilities for access and delivery of knowledge to the users.

> Numerous initiatives are addressing IDM on an individual basis. A critical part of accomplishing the IM mission as set forth in this document is implementing IDM in a thoroughly integrated fashion. Therefore, IDM supporting the Global Broadcast

> Service (GBS) program will be used as a baseline with the expanded IDM effort led by USACOM used to guide all future IDM development. All organizations will ensure their IDM related activities are integrated with and are compatible with the current IDM effort.[21]

The fourth objective for the second goal is to "introduce new paradigms." How can the Army take advantage of the rapidly developing technology and deploy it in a timely manner? Capabilities and the potential of technology are advancing more rapidly than ever. Computers advance at an exponential rate according to Moore's Law. Computer history over the past 30 years provides support data for Moore's Law, there is no reason to think this rate will slow in the near future. The Army no longer has the time to slowly implement new technology into the organization. During the Cold War era, parallel running of new and old systems to allow personnel to "get accustomed to" the new system could be considered. This is a luxury the Army can no longer afford.

Although technology is "tempting," the Army must be careful not to buy technologies that can not be deployed in a timely manner nor, will not fit the existing environment. Modeling and simulation will be needed to ensure the rapid employment and smooth integration of new systems. In the past, new systems were developed or purchased without full consideration of the impact on the existing architecture. The practice was to deploy the new system and then fix the glitches as they appeared. This has lead to the data inaccuracies the Army currently has, and is very costly to correct.

The current military directive is to purchase COTS products whenever possible. It is thought that this will encourage local, small and disadvantaged vendors to develop IT products and services in a competitive environment. In this way the Army can take advantage of the leading, bleeding edge of technology without having to pay for research and development. By obtaining models of the new systems and products from the contractors, the "fit" of the product into the existing architecture can be tested before deployment. Time is saved in the

documentation of the new systems into the enterprise architecture since the models and fit have already been tested. Training on the new system should be accomplished through the Distance Learning Program. Contracts for new systems should always include the requirements for both modeling of systems and the training of users. When planning for training, all personnel (military, civilian, and contractors) need to be considered.

The fifth objective, "improve IT management tools," for Goal 2 hints at modeling and simulation, media methods, and other information management assets. In order to improve, or increase your tools, you must first know what you have. Defining the architecture of the enterprise organization is key. Using organizational models will identify links to other organizations as well as to the mission. By using modeling and testing of new systems before they are installed the process owners and the CIO can see where process improvements, impacts, or adjustments need to be made.

The terrorists succeeded in their attack on September 11th due to the Nation's weakest link, the lack of integrated information access. Future attacks will only be thwarted through the rapid exchange and analysis of information from all methods and media. Integration of information access and management methods for all media and types of information should be a priority. The DoD IM Strategic Plan suggests that the transformational user requires automated, streamlined methods to access information routinely and reliably. A common semantics, syntax, and procedures set would include electronic directories. Examples of these are already in development, such as the Government Information Locator Service (GILS), Defense Data Dictionary System (DDDS). A secure message exchange system for Defense Messaging System (DMS), and World Wide Web (WWW) information providers is a must.[22]

To be able to take full advantage of IT management tools the Army must be able to locate and track what it already has. Only by tracking when a tool is at the end of its life-cycle

can it be planned for replacement. The replacement process also needs to be timely, efficient and tracked. DoD has initiated a Defense-wide IT Total Asset Visibility (ITTAV) universally.

> The ITTAV concept can be used to manage IT "objects" like hardware, software, and data for the user throughout their life cycle. ITTAV "tracking" includes tracking the status of user orders for IT objects, maintaining accurate inventory records, automatically ordering upgrades, and managing asset reuse and removal.[23]

Through good customer-supplier communications and contracting, hardware, software, and IT services can be treated like any other raw material. The key here is in the procurement phase of the process. By writing the life-cycle replacement and upgrade needs into the contracts, future programming requirements can be projected. When programming resources during the POM cycles, this action will facilitate an efficient interface with existing systems and processes.

GOAL 3. REFORM IT MANAGEMENT PROCESSES TO INCREASE EFFICIENCY AND MISSION CONTRIBUTION.

Office of Management and Budget (OMB) in its circular A-130 requires agencies to develop a business case for every IT investment. These cases must include performance goals and measures, process controls, security features and a plan for integrating the new system with the enterprise architecture. As the Army role and configuration transforms for the future threat requirements, information and technology will be more important. Therefore, information and information technology from an Army-wide perspective must be managed as a strategic resource. The Army must base information and IT decisions on their contribution to the effectiveness and efficiency of military missions and supporting business functions.

The DoD definition for Goal 3 stresses the importance of managing IT resources and aligning strategies and programs with Defense-wide, functional, and organizational goals and

measures. IT performance measures and contribution to the mission must be assessed in the context of the functional and organizational performance plan.

> IT portfolios investments must be linked to mission goals, strategies, and architectures, using various assessment and analysis tools. Information management, itself a business function, must employ best business practices to continuously improve customer/user support, reduce infrastructure costs, and apply the best available information technology.[24]

The first objective that DoD has stated to support Goal 3 is to "institutionalize the Clinger Cohen Act (CCA) provisions." The CCA demands that the existing processes be analyzed to ensure stovepipe systems and processes are not perpetuated. In the quest for "systems thinking," organizations must examine their strengths, weaknesses, opportunities, and threats. If the Army is successful in disseminating its vision and mission down to all levels, it will be evident by the emergence of new strategic issues. Personnel at any level will be able to recognize and push forward any idea for a process change. Business process reengineering (BPR) or improvement (BPI) requires a champion to drive change. Change must be driven by top management, but can only be achieved with corporate buy-in. To achieve this "executive improvement teams (EITs) should be involved in setting the priorities of the process improvement plan, appoint process owners, and monitor progress." [25]

There are already organizations established to manage process and IT changes. The issue is that complete and proper representation is not always present. For example, the Defense Integrated Management of Human Resources System (DIMHRS), a system that has been in ongoing development for many years, has not been able to stabilize people in the project office. The system vision is to establish one Human Resources system for all of DoD so the frontline commanders have the ability to find personnel with necessary skills. The Army has embraced the vision with one of their own, ITAPDB as mentioned previously, which will incorporate all of the Army components' personnel management systems. Currently there are over 300 Army personnel systems used to hold data for various personnel reporting purposes. Efforts to change processes

and the IT support for them are hampered by each Army component seemingly unwilling to compromise on the data format needed for their specific reporting issues. This lack of cooperation is a microcosm of the change effort facing the Army and DoD in its Transformation.

Changes in the personnel systems will cause changes to the personnel management processes; yet no effort has been made to adjust the types and frequency of the reports to Congress. Many of these reports are outmoded. The current report processes have roots, which date back to the Korean and Vietnam War days. Many stovepipe systems have also been developed as a result of each Army component's justification of different reporting requirements. There have been many developments in recent years in the field of human resource management, yet the Army has not fully embraced the best practices in this area.

Once the processes have been identified, a champion selected, and objectives and milestones set by the committees, modeling of the new process can take place. Sometimes it will become necessary to run the old business processes parallel to the new ones to achieve full buy-in to the change. This can also prove the validity of the new process as compared to the old one. Most importantly, running parallel systems allow users to gain a certain amount of confidence in their individual abilities in operating the new system.

DoD uses the term "applications implementation" to describe the enterprise-wide migration of systems. This aligns applications support with functions and processes. Examples can be taken from the personnel area where committees have been formed to link the human resource processes with the POM process. There needs to be continued emphasis on implementing applications to support reengineered processes that achieve mission and functional goals. Performance measures on COTS software should be used to the maximum extent possible for verification of the product. Information support providers, both in-house and contractors, must maintain a program of continual improvement linked to user requirements, software best practices, and the software capability maturity models.[26]

In order to have seamless application implementation, strategic planning must be coordinated between the functional community and the CIO. The ideal way to achieve this is through a thorough and defined strategic planning process. Using tools like Robert Kaplan's Balanced Scorecard, the organization can identify the core processes and analyze the need for any business process reengineering that should occur. The IT should not drive the analysis or the mission. After the mission assessments and analysis is done, the CIO will assist in linking the IT to the mission. It is vital to align IT investment decisions to support improved mission processes.

In the Army Reserve, processes have already been put into place to better link the investment decisions with the mission processes. A committee in the personnel area, the Reserve Personnel Systems Integration Group (RPSIG), has been established to examine all IT change requests and proposals that impact on the personnel systems and processes. This group has representation from the various Reserve organizations, the CIO, and the CFO. The group ensures that strict mission accomplishment and process improvement are the basis for any decision for IT money requests. Only after the request goes through this committee does it go before the Council of Colonels and then the POM board for funding requests.

Customer or user focus begins with the strategic linking of the mission, and IT, to the budget. There are tools developed by private industry to help facilitate this process. The requirement here is for the Army to choose a tool and use it as a standard for the functional community to use.

> Tools and policy will help activities systematically introduce and maintain customer awareness and compare their performance with peers. In industry, customer focus is routinely practiced and supports continuous improvement of processes, practices, and people. Routine use of customer surveys by IT organizations to measure satisfaction at all levels is a key approach.[27]

Best practices, or benchmarking, taken from private industry can be widely used here. A best practices agenda calls for the following:

- Make sure you know all links in your value chain.
- Establish a competitive pricing strategy.
- Develop strong advertising strategies.
- Train your employees to know the products/processes and the customers that use them.
- Develop an integrated system for processing orders tailored to customers' needs.
- Do business with the customers you choose and in the ways you choose.[28]

The second objective in support of Goal 3 is to "institute fundamental IT management reform efforts." The Army must take examples from private industry in order to survive the reforms that have already taken place with the GPRA and CCA. By mimicking best practices used for the faster-paced private industry, the Army can establish standardization for measures and assessments in IT.

> Performance measures linked to mission need to be embedded systematically at all levels of The Army including local activities and IT staffs. While the focus is on organizational improvement, both Capability Maturity Models (CMM) and Baldrige criteria, for example, provide quantitative assessment methods that can be used as performance indicators.[29]

The use of milestones during the IT project process and the periodic review of the requirements as laid out in the statement of work (SOW) can help keep the project on track. If the IT system is already in place, a review of the mission linkage through the Baldrige or Balanced Scorecard methods can identify if the system has any remaining value to the organization.

Using other services and private industry as examples for benchmarking, the Army can use these lessons learned to improve its IT business processes. A "comprehensive, time-phased plan for assessing and improving all IT processes, including strategic planning, policy and policy enforcement, requirements generation, programming and budgeting, acquisition, and operations"[30] can be attained using strategic planning methods.

New books on improved methodology and tools for project management come out almost daily. DoD has institutionalized some of these such as: BPR, benchmarking, Total Quality Management (TQM), architectures and other improvement activities. "These and other

tools must be integrated into the actual life-cycle so end-users, managers, and developers can apply them easily, routinely, and incrementally."[31]

Institutionalizing IT project management is slightly different than other types of project management. The following steps outline IT project management:

Step 1: Determine technology opportunities.
Step 2: Define the long-term new systems and technology architecture.
Step 3: Sequence the IT projects and the implementation of the new architecture.
Step 4: Evaluate and select the vendors and the products for the new technology.
Step 5: Develop the project plan for implementing the technology.
Step 6: Carry out the technology project.
Step 7: Measure the results of the project.[32]

Goal 3's third objective is to "promote the development of an Information Technology Management (ITM) knowledge-based workforce within the Army." The Army spends much of it resources on the recruitment and training of personnel. The most highly trained personnel are those in the specialties of acquisition and information technology/management areas. The Army can not afford to send personnel to training only to have them leave for higher paying jobs with private industry. Collaborating with private industry in programs like "training with industry" can provide a win-win partnership. The goal is that industry gets a highly disciplined government person to work on a project and the Army gets back a better-trained and more experienced "employee."

A major issue in keeping a trained IT person is that private industry pays better. So what can the Army do to remain competitive with private industry so that soldiers will want to stay? One way to entice personnel to stay is to create better job satisfaction within the IT community. Human resource management is currently making changes in the area of recruitment and placement of skilled IT personnel. In the past, personnel were placed in positions according to the organizational need and not necessarily based on schooling or skills. The Reserve, for example, has created a new combined office to review credentials and ensure that properly trained and experienced personnel are placed in IT and acquisition positions.

Training, whether it is with the Army or from private industry, is valuable. Validating and keeping track of personnel skills assessment is becoming more important than ever. Using organization and individual assessment tools to determine skill requirements and maintaining an IT personnel skills database to document skills, including skills obtained from private industry and courses, needs to be maintained in the human resource area. The newly formed Reserve office uses tools such as surveys, self-assessment, and board processes to determine skill levels of personnel. Surveys and organizational mission requirements are used to place the personnel in organizations for the "best fit."

All personnel need training on various systems they will be using for their positions. The Army must provide training and educational opportunities to its personnel. IT projects and procurements should take into account training of personnel on the new system. Contracts with vendors can be written to accomplish training at the installation of the new system, at any upgrade or improvement, and periodic training to train newly arrived personnel.

The fourth objective for Goal 3 is to "provide the IM/IT support required to ensure individuals with disabilities have equal access to the information environments and opportunities in the Army. DoD has developed the Computer/Electronic Accommodations Program (CAP)." New directives and laws have been established that required all Internet portals to be handicap compliant by Oct 2001. The Army portal, AKO, is in compliance. Technologies in use today for the Army's disabled employees include voice recognition, eye tracking, handwriting recognition software, as well as large-format displays. Individual needs should be addressed and available technology used to provide the best possible work environment for personnel.

The fifth objective for DoD's third IM goal is to "integrate the Army IT activities." Providing standardized IT policies and procedures for the Army should be done in cooperation with other organizations that have a stakeholder interest in IT. Guidance can be tailored for various missions. Due to globalization, threats that were once contained to specific geographic

areas are now showing up in other countries. During the Cold War there was a defined opponent to be faced on a predictable battlefield; but with the fall of the Wall and the September 11th attack the National Defense Plan has changed its focus. Terrorism is one threat that knows no boundaries. To be sure, there is not going to be a "one-size-fits-all" IT solution to all possible missions to fight terrorism. However, information policies can be made flexible enough to be able to take advantage of IT advancements so they can be used to leverage the Army's dominance of the situation. Scenario planning and modeling and simulations can greatly assist in the innovative uses for technology.

Wherever possible, IT solutions should be based on multi-agency functions that should link readily, rather than on project or agency specific ideas. Public-private partnerships should be formed to ensure that IT solutions to problems built in the private sector could be built on for the public sector without having to start from scratch. These partnerships should stretch across all domains of research and development, pilot programs, and standards.

> Identify the relationships between IT applied in different domains to ensure that overarching objectives such as interoperability, information security, and efficiency are met; and mission threads, such as sensor-to-shooter, are effective. Dependencies such as those between IT activities in support missions (e.g., procurement, personnel) and the common infrastructure will be described and strategies for managing them established. Interoperable IT is integral to the effectiveness of our weapon systems.[33]

In creating partnerships the Army must also consider the subcontractors. This outsourcing chain of responsibility can expedite the IT projects or hamper them. Outsourcing can be thought of as a form of delegation. However, as with any other time something is to be delegated to another party, the underlying principles of responsibility, accountability, and authority should be thoroughly outlined. If outsourcing is done with only cost cutting in mind, then "problem fixing" must also be taken into account. Inevitably, cost-driven outsourcing policies have proven to be inefficient since a large number of subcontractors are costly to manage. New guidelines are emerging that will clarify criteria for outsourcing. Barriers to

outsourcing, such as A-76 and lengthy cost studies, are being rewritten so as to clarify and expedite the ability to outsource. Any case for outsourcing needs to be fully analyzed and integrated within an overall strategic IM process. In any outsourcing endeavor current resources, as well as the question of what is "inherently governmental responsibilities," must be addressed. Inherently governmental responsibilities as outlined in the Office of Management and Budget (OMB) Circular A-76, Policy Letter 92-1 are:

> A function that is so intimately related to the public interest as to mandate performance by Government employees. Governmental functions normally fall into two categories: (1) the act of governing, i.e., the discretionary exercise of Government authority, and (2) monetary transactions and entitlement. An inherently governmental function involves the interpretation and execution of the laws of the United States. [34]

GOAL 4. ENSURE THE DOD'S VITAL INFORMATION RESOURCES ARE SECURE AND PROTECTED.

Information is vital to the operations of the Objective Force and should be a protected resource. Information Assurance (IA) is essential to integrate intelligence, command and control, and battlefield awareness functions into joint and combined operations. IA is crucial element in implementing protection of critical national infrastructures as mandated by the Presidential Decision Directive – 63, Critical Infrastructure Protection. But, integration involves more than simply acquiring IA technology. It requires improving the understanding and awareness by individuals throughout the Army of information operations criticality, and the impacts of an inadequate IA posture on defense missions. This requires recognition that IA is a warfighting concern and ranks appropriately in command attention and budgetary tradeoffs with other warfighting capabilities.

A robust IA program requires:

- Concept of operations.
- Continuous monitoring and assessment of threats, vulnerabilities, and readiness posture.

- Appropriate architecture, technology, tools, and material.
- Sufficient numbers of adequately educated and well-trained personnel.
- Effective operational policies and doctrine.
- Appropriate management and oversight.
- The ability to quickly and efficiently implement agency-wide security measures and countermeasures to limit damage when threatened.[35]

The first objective for DoD's fourth goal is to "make IA an integral part of DoD mission readiness criteria." The first step toward this objective is to identify the systems and their importance in the GIG. These systems fall under one of three categories; mission critical, mission essential, or mission support. Ideally the identification and classification of the systems is done during the strategic planning phase. During the documentation of the enterprise architecture, all mission critical data elements, information systems, and their operational necessity should be identified. Periodic reviews and updates of all three areas of the architecture (operational, technical, and systems) will ensure that mission link will remain constant.

The second step to achieve this objective is to provide IA levels consistent with the DoD's mission critical, mission essential, and mission support requirements for all networks on the GIG. The Army envisions a "Defense-in-Depth" strategy for information assurance. This consists of several layers of defense based on the technical and operational architecture. Intrusion detection systems, consisting of firewalls and other high-security measures to guard software and hardware, are placed on the perimeters of the network. Internal barriers also include firewalls and router filtering devices. These serve as barriers between organizational levels and other functional communities.

The third step in making IA an integral part of the Army and DoD mission readiness criteria is to integrate IA readiness standards and metrics into the Army readiness reporting process. In the book *Information Warfare*, the author Winn Schwartau states:

> In the United States the National Security Agency sets the standards by which computer security is measured.[36]

The Information Operations Condition (INFOCON) process has been established to provide standard guidance for actions to defend against network attacks. It also provides a reporting criteria, response actions, and counter measures for cyber attacks on computer, and telecommunication, networks and systems. There are five levels of defensive posture, which are established by the Secretary of Defense and administered through the operations staff (J3 – S3). Subordinate and operational commanders may increase the level of INFOCON, but cannot lessen it.

The second objective for Goal 4 is to "enhance DoD personnel IA awareness and capabilities." To achieve information superiority everyone must understand the value of information and the enterprise architecture it resides on. This is done through a comprehensive training and certification program. In *Information Warfare*, Winn Schwartau states:

> Anyone can be an Information Warrior. An unhappy worker, a government employee, or a teenager at the family PC, are all potential Information Warriors. Information Warfare (IW) is about capabilities, the potential power of the individual and the potential power of an organized group.[37]

Security is only as good as your weakest link. Only by educating everyone can there be an understanding of the potential threat. When people understand a threat can come from anywhere at anytime, they can be more vigilant and are apt to more rapidly report any abnormality. Currently, regularly scheduled security briefings are in place to educate and remind personnel of the importance of IA. Periodic training can be programmed into the network, so when a person signs onto the system a short refresher training has to be performed before the login process continues. This training and awareness must include all supporting agencies to the Army. The requirement for IA education and periodic awareness classes should be written into vendor contracts. Strict adherence to IA should also be a performance measurement in any contract.

IA is a specialized field within the IM community. Military and civilian personnel may need special security clearances and accreditations on training needed for this field. An office within the CIO has been established for IA. Personnel training and career management are being closely monitored by the newly formed office within the Army Reserve Personnel Command. The Army has the responsibility to create new career fields as technological changes occur. As the DoD IM Plan states:

> Career field designation is essential to establishing ascension paths for the military and civilian disciplines critical to ensuring efficient secure operation of the GIG.[38]

The third objective for Goal 4 is to "enhance DoD IA operational capabilities." DOD calls for a Defense in Depth concept to accomplish this goal. A secure perimeter and an integrated attack sensing and response management system are essential to this concept. This concept has been adopted by the Army, and is applied to each operating assurance level in accordance with DoD criteria, including existing protective measures. This concept consists of the following:

- Hardened network infrastructure.
- Protected host secure operating systems.
- Protected enclave boundaries.
- User/Application layer security services, including non-repudiation, signature, integrity, and confidentiality.
- Employment of strong identification and authentication (I&A) services.
- Use of a common, integrated Army Public Key Infrastructure (PKI) to enable security services at multiple levels of assurance.
- IA situational awareness based on both network and host monitoring to formulate and support an attack sensing and response management capability.
- Approved high assurance devices and configurations for all interconnections among mission sensitivity levels.[39]

The Defense-in-Depth concept is employed to ensure a well-controlled perimeter. Constant upgrading of the perimeter firewalls is necessary to prevent unwanted intrusion from outside personnel or agencies. Authentication methods are being improved at an accelerated rate; however, cost is still prohibitive. The Public Key Identifier (PKI) project has been making steady progress. This program will enhance the privacy and security technology developments

designed to validate user identification through digital signature certificates. New efforts are underway to apply biometrics to safeguard systems against illegal or forced access. Intrusion detection systems (IDS) are installed at the perimeter of the network and key servers to safeguard the Network. IA architecture, connection standards and procedures are being established. The Army has employed the INFOCON system and established the Army's Information Systems Security Program (AISSP) under the Information Assurance Directorate in the G-6 office. The Network Security Improvement Program (NSIP) Plan outlines the sustaining base for the Army.

The final objective for DoD's fourth Goal is to "establish an integrated DoD security management infrastructure (SMI). The documentation of the Army's Enterprise Architecture (AEA) provides the picture of the information grid so the Information Assurance Directorate can develop the security program plan. The AISSP program has the responsibility for the plan to protect the network perimeter from intrusion. It also provides the ability to react to intrusion in a coordinated effort.

Having looked at the DoD IM Strategic Goals and objectives, the next step in the planning process is the implementation. The procurement of required technology is linked to the success of the implementation. These processes will be discussed in the next section.

PLANNING IMPLEMENTATION AND PROCUREMENT PROCESS

The area where most strategic plans fail is in the implementation phase. Turning strategy into executable actions and results is a feat that seemingly eludes many organizations. Due to the relatively rapid turnover of personnel, visions, and consequently plans, change. In James Higgins and Julian Vincze's book, *Strategic Management*, they outline four issues that need to be addressed in the implementation of a strategic plan.

> Four primary issues are involved in implementation: structuring the organization; employing appropriate implementation systems; adopting the proper management style; and managing organizational culture (shared values). Implementation is now recognized as critical to the success of strategic management.[40]

The *DoD Information Management Strategic Plan Guidance* outlines the IM strategic planning process; the Guiding Principles, including the Strategic Planning, Implementation Planning, and Performance Guidelines; IT Performance Measures; and the DoD IM Strategic Plan Linkage with the Planning, Programming, and Budgeting System (PPBS).[41] However this guidance is high level guidance and leaves it up to the services to develop their own specific IM plans and programs for implementation.

DOD STRATEGIC PLANNING:

A quick explanation of the DoD Strategic Planning diagram follows.

> The IM planning flow is highlighted in Figure 2 in the context of other strategic planning and links to programming. The President's National Security Strategy drives the formulation of the National Military Strategy (NMS) by the Joint Chiefs of Staff (JCS). *JV2010* articulates the Chairman's future concepts for joint military operations. The *QDR,* under the leadership of the Secretary, defines the goals and major strategies for the Command to move into the 21st century. It shows how the Command will exploit the Revolution in Military Affairs (RMA) and the Revolution in Business Affairs (RBA). The *QDR* is DoD Strategic Plan that responds to the GPRA of 1996. Under this capstone guidance, principal staff assistants (PSA's) prepare functional strategic plans for their assigned areas of responsibility such as logistics, finance, health, and personnel. Organizations prepare visions and strategic plans to accomplish their organizations' missions and functions. DoD IM Strategic Plan is aligned with DoD, functional, and Organizations visions/plans to ensure that DoD IT optimally supports the entire Defense mission. IM guidance is included in the Defense Planning Guide (DPG). Organizations prepare POM inputs, which balance all guidance and requirements. Office of the Secretary of Defense (OSD) reviews POM inputs to ensure they satisfy DPG and other guidance such as the DoD IM Strategic Plan. The budgeting processes lead to an authorized defense program.[42]

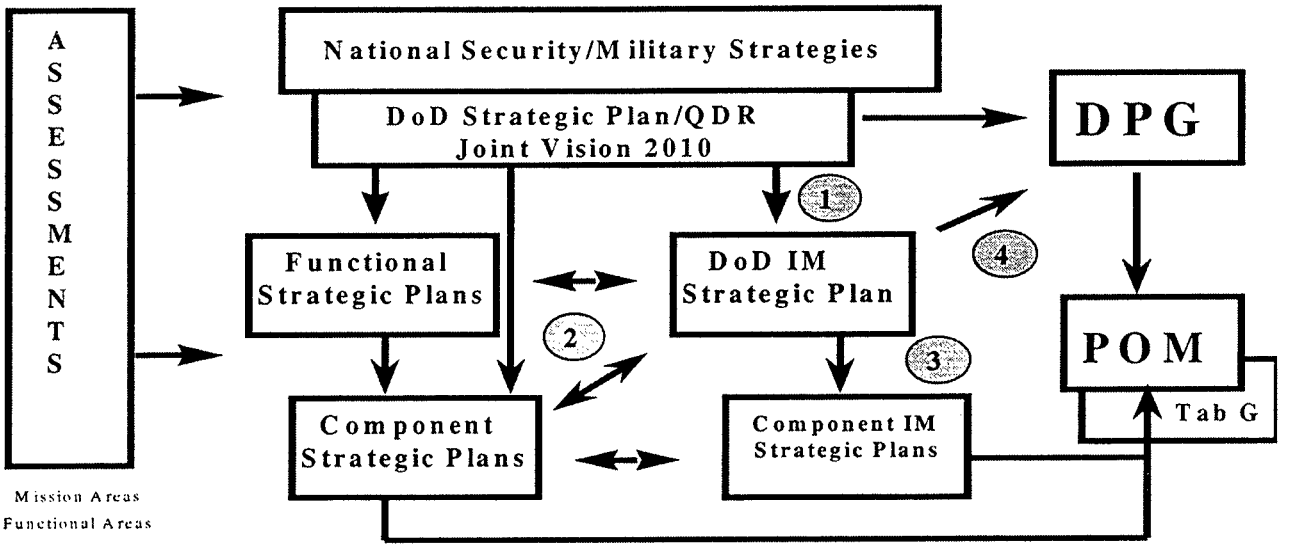

FIGURE 2. THE DOD IM STRATEGIC PLANNING FLOWS AND LINKS

As shown in the figure above, the four key linkages (labeled 1-4) between The DoD IM Strategic Plan are:

1. The DoD Strategic Plan/*QDR* and *JV2010*
2. Functional and Organizations strategic plans
3. Organizations IM Strategic Plans, and
4. The DPG and the POM Tab G. [43]

Each sub-organization is responsible for the linkage to the higher Headquarters' Strategic Plan. Component CIO's will develop the IM strategic plans to link to the Joint, DoD, and Army IM strategic plans.

Figure 3 (next page) shows the IM strategic planning cycle. This schedule synchronizes the IM planning cycle with other strategic planning cycles and timelines.[44]

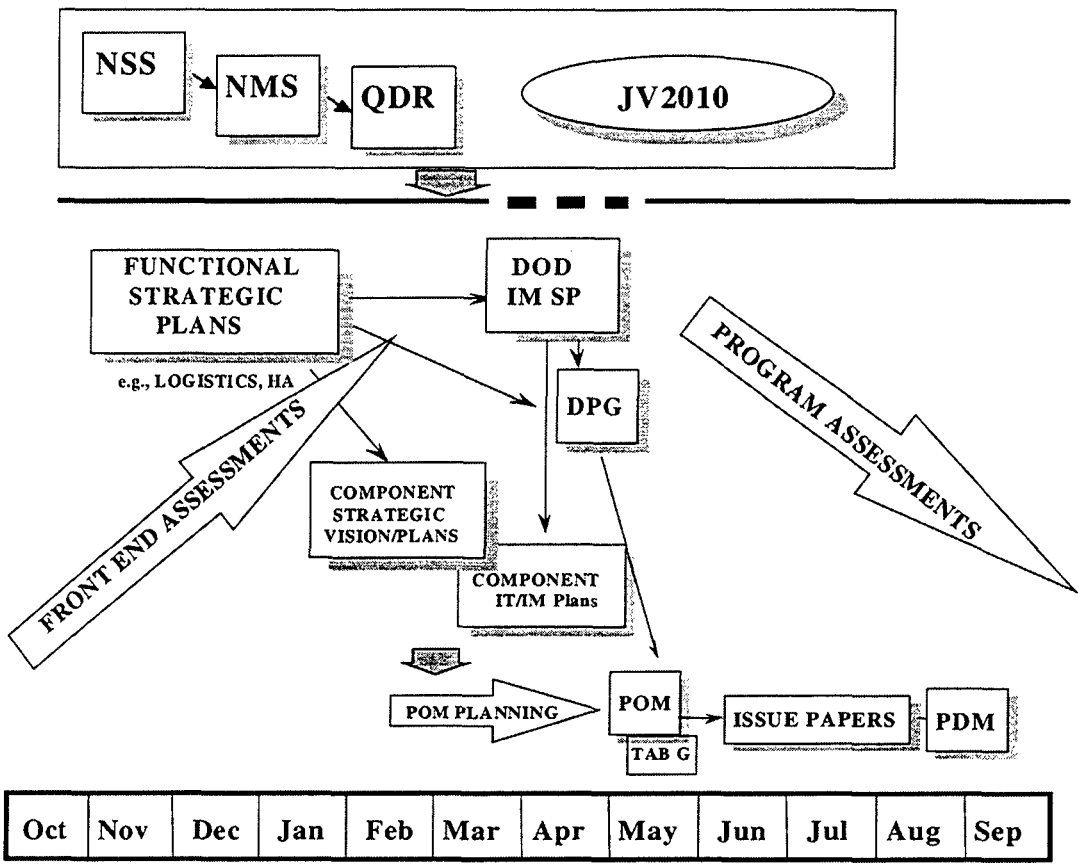

FIGURE 3. IM PLANNING CYCLE

INFORMATION TECHNOLOGY INVESTMENT PORTFOLIO OVERSIGHT

Another shortfall in the IM implementation phase is in the oversight of the IT investments. As stated earlier, almost one-third of the defense budget is in IT investments. According to DoD, these shortfalls are due to the following:

1. Minimal linkage between IT investments and functional direction/process changes.
2. Individual systems narrowly focused on specific functions and organizations vice total mission.
3. Fragmented systems and infrastructure result in a lack of fully integrated and interoperable capabilities.[45]

The new acquisition reforms should be fully implemented at all levels.

> Improved acquisition initiatives must fully integrate the efforts of the Joint C2 Integration and Interoperability Group (JC2I2G), the CINC Interoperability Program Offices (CIPOs), the Joint Forces Program Office (JFPO), the Joint Forces Command (JFC), and the Joint Staff to establish a joint Command, Control and Communication (C3) integrated system development process that emphasizes "joint first". Promising concepts and technologies from research experiments, pilot projects, and operational demonstrations must be moved through the acquisition process smoothly and efficiently. New paradigms of acquisition must be exploited that expedite the use of COTS (e.g., the Federal Acquisition Regulation (FAR) Section 12, new testing rules for COTS), exploit commonalties (e.g., product lines), and provide insight into front-end processes (e.g., ACTDs) and other initiatives (e.g., Global Combat Support System (GCSS)).[46]

The new acquisition reforms are combining technical, financial, negotiating, and administrative processes into a single, dynamic process for systems acquisitions.

The Chief Finance Office (CFO) and the CIO have partnered to develop a process to correct these shortfalls. For example, the Army Reserve has developed a process consisting of a series of committees that meet regularly to review and vote on system changes. This process is supported by an IT system called the Service Request System (SRS). In using this system, change requests to systems are captured, supporting documentation is attached, and a champion is assigned. The request is forwarded to the service provider for an estimate on the time and cost to work on the change. When the request is brought before the functional user committee a full accounting of how much money allocated to the particular system is shown. The committee can then decide to spend the money to make the recommended changes or divert the money to a more critical change on another system.

There are two committees set up within the Army Reserve Personnel Command. The first is the Working Committee, which consists of the functional process owners and the Directorate Information Management Officers (IMOs). The CIO chairs this committee. The higher committee is the Steering Committee, consisting of the Directors. These are the champions on the systems and processes, and the organizational decision makers. The Deputy Commander of the organization chairs this committee.

Before the IT requirement action is closed the requester must approve the service provider product. The requester must then adequately test the new or changed system to ensure that it meets the functional need. Once the requester approves the product, the service provider updates the SRS to show requirement completion.

IT procurements under $5000 do not normally require the committees' approval, but still must be tracked for command IT resource monitoring. Therefore, the Commander, Deputy Commander, or Chief of Staff must approve all IT purchases. Any IT purchases over $5000 go to the committees for approval.

Using this committee method, the organization has visibility and voting rights over the IT dollars spent. If a change to a system is required, a quick committee meeting is held to determine if there is enough money in the IT "checkbook" to cover the change, or if the money needs to be migrated from another system's resources to cover the expense. If there is not enough money left in the organizational IT budget, a quick determination and a request for funding is sent to the POM process as soon as possible. It is envisioned that in the future the SRS will be expanded so emergency committee meetings can be held electronically. This will save even more time and money by adding IT efficiency to the process.

SUMMARY

Readiness is the Army's main concern. Without accurate, reliable, and timely information the Army cannot fulfill its role in the national strategy. The best, most accurate data is that which comes directly from the source. By creating a secure portal that customers can access, see the information they require, and use the information for improving the knowledge base, the Army can greatly improve its information superiority. The extent of the customer access to the data needs to be determined by strategic analysis and planning. Risk analysis

results need to be weighted for return on investment against the risk of electronic security and privacy.

As the Army moves forward in its Transformation, it is increasingly important for all components of the organization to create a partnership to enhance IM resources. Only by examining the core competencies, documenting the enterprise architecture, and analyzing the current level of resource management compared to future needs can the Army move forward into the Information Age. Information dominance is the key to successful operations on the 21st Century battlefield and beyond. IT is the critical enabler to achieve the Army's Transformation Strategy and a secure, robust information infrastructure linked securely with the mission and the funding process is an absolute.

WORD COUNT = 10,287

ENDNOTES

[1] Department of Defense (DoD) Chief Information Officer (CIO). Information Management (IM) Strategic Plan; Information Superiority, Version 2,0. (np: October 1999.), 15.

[2] Ibid., 6.

[3] Peter Rea, Ph.D. and Harold Kerzner, Ph.D., Strategic Planning a Practical Guide, (New York, New York: John Wiley & Sons, Inc., 1997), 2.

[4] Department of Defense (DoD) Chief Information Officer (CIO). Information Management (IM) Strategic Plan; Information Superiority, Version 2,0. (np: October 1999.), 21.

[5] Bennet P. Lientz and Kathryn P. Real, Breakthrough Technology Project Management., Second Edition. (San Diego, California: Academic Press, 2001), 21-22.

[6] Department of the Army. Joint Technical Architecture – Army, Version 5.5, (Washington, DC, December 1998), 2.

[7] Department of the Army. Enterprise Architecture Guidance Document (AEAGD), Version 1.1, (Washington, DC, Dec 1998), ES-1.

[8] Department of Defense (DoD) Chief Information Officer (CIO). Information Management (IM) Strategic Plan; Information Superiority, Version 2,0. (np: October 1999.), 22.

[9] Ibid.

[10] Peter Rea, Ph.D. and Harold Kerzner, Ph.D., Strategic Planning a Practical Guide, (New York, New York: John Wiley & Sons, Inc., 1997), 41.

[11] Department of Defense (DoD) Chief Information Officer (CIO). Information Management (IM) Strategic Plan; Information Superiority, Version 2,0. (np: October 1999.), 22.

[12] Arthur Andersen, Robert Hiebeler, Thomas B. Kelly, and Charles Ketteman. Best Practices; Building Your Business with Customer-Focused Solutions. (New York, New York: Simon & Schuster, 1998), 176.

[13] Department of Defense (DoD) Chief Information Officer (CIO). Information Management (IM) Strategic Plan; Information Superiority, Version 2,0. (np: October 1999.), 22.

[14] Ibid.

[15] Larry P. English. Improving Data Warehouse and Business Information Quality: Methods for Reducing Costs and Increasing Profits. (New York, New York: John Wiley & Sons, Inc., 1999), 26 – 60.

[16] Yogesh Malhotra. "Knowledge Management for E-Business Performance: Advancing Information Strategy to 'Internet Time'". Information Strategy, The Executive's Journal. Vol. 16 (4), Summer 2000, 6.

[17] Department of Defense (DoD) Chief Information Officer (CIO). Information Management (IM) Strategic Plan; Information Superiority, Version 2,0. (np: October 1999.), 24 –25.

[18] Brad L. Peterson, and Diane M. Carco. The Smart Way to Buy Information Technology: How to Maximize Value and Avoid Costly Pitfalls. (New York, New York: American Management Association, 1998), 118.

[19] Department of Defense (DoD) Chief Information Officer (CIO). Information Management (IM) Strategic Plan; Information Superiority, Version 2,0. (np: October 1999.), 25- 26.

[20] Ibid., 26.

[21] Ibid., 27.

[22] Ibid.

[23] Ibid.

[24] Ibid., 28.

[25] H. James Harrington. Business Process Improvement: The Breakthrough Strategy for Total Quality, Productivity, and Competitiveness. (New York, New York: McGraw-Hill, Inc., 1991), 19.

[26] Department of Defense (DoD) Chief Information Officer (CIO). Information Management (IM) Strategic Plan; Information Superiority, Version 2,0. (np: October 1999.), 26.

[27] Ibid., 29.

[28] Arthur Andersen, Robert Hiebeler, Thomas B. Kelly, and Charles Ketteman. Best Practices; Building Your Business with Customer-Focused Solutions. (New York, New York: Simon & Schuster, 1998), 132 – 133.

[29] Department of Defense (DoD) Chief Information Officer (CIO). Information Management (IM) Strategic Plan; Information Superiority, Version 2,0. (np: October 1999.), 29.

[30] Ibid.

[31] Ibid.

[32] Bennet P. Lientz and Kathryn P. Real, Breakthrough Technology Project Management., Second Edition. (San Diego, California: Academic Press, 2001), 220 – 221.

[33] Department of Defense (DoD) Chief Information Officer (CIO). Information Management (IM) Strategic Plan; Information Superiority, Version 2,0. (np: October 1999.), 30.

[34] Office of Management and Budget. OMB Circular A-76, Appendix 5: Office of Federal Procurement Policy (OFPP) Policy Letter 92-1, "Inherently Governmental Functions." (np: September 23, 1992), 2.

[35] Department of Defense (DoD) Chief Information Officer (CIO). Information Management (IM) Strategic Plan; Information Superiority, Version 2,0. (np: October 1999.), 31-32.

[36] Winn Schwartau. Information Warfare; Cyberterrorism: Protecting Your Personal Security in the Electronic Age. (New York, New York: Thunder's Mouth Press, 1996), 668.

[37] Ibid., 39 – 40.

[38] Department of Defense (DoD) Chief Information Officer (CIO). Information Management (IM) Strategic Plan; Information Superiority, Version 2,0. (np: October 1999.), 33.

[39] Ibid., 33.

[40] James M. Higgins and Julian Vincze. Strategic Management, Text and Cases. (New York, New York: The Dryden Press, 1989), 7.

[41] Department of Defense (DoD) Chief Information Officer (CIO). Information Management (IM) Strategic Plan; Information Superiority, Version 2,0. (np: October 1999.), Section V. and Appendixes A – E, 35 – 54.

[42] Department of Defense (DoD) Chief Information Officer (CIO). Information Management (IM) Strategic Plan; Information Superiority, Version 2,0. (np: October 1999.), 42.

[43] Ibid., 43.

[44] Ibid., 46.

[45] Ibid., 48.

[46] Ibid., 29.

ACRONYMS

ACTD	Advanced Concept Technology Demonstration
AEA	Army Enterprise Architecture
AEAGD	Army Enterprise Architecture Guidance Document
AISSP	Army Information System Security Program
AKO	Army Knowledge Online
AMC	Army Material Command
AWE	Advanced Warfighting Experiment
BPI	Business Process Improvement
BPR	Business Process Reengineering
C2	Command and Control
C3	Command, Control and Communications
CAP	Computer/Electronic Accommodations Program
CCA	Clinger-Cohen Act of 1996
CFO	Chief Financial Officer/Office
CIPO	CINC Interoperability Program Office
CINC	Commander in Chief
CIO	Chief Information Office/Officer
CMM	Capability Maturity Model
COTS	Commercial-Off-the-Shelf
DDDS	Defense Data Dictionary System
DIMHRS	Defense Integrated Management of Human Resources System
DMS	Defense Messaging System
DoD	Department of Defense
DPG	Defense Planning Guidance
EIT	Executive Improvement Teams
FAR	Federal Acquisition Regulation
GBS	Global Broadcast Service
GCSS	Global Combat Support System
GIG	Global Information Grid
GILS	Government Information Locator Service
GPRA	Government Performance and Results Act of 1993

IA	Information Assurance
IDM	Information Dissemination Management
IDS	Intrusion Detection System
IM	Information Management
IMO	Information Management Officer
INFOCON	Information Operations Condition
IT	Information Technology
ITAPDB	Integrated Total Army Personnel Database
ITM	Information Technology Management
ITTAV	Information Technology Total Asset Visibility
IW	Information Warfare
JC2I2G	Joint Command and Control Integration and Interoperability Group
JCS	Joint Chiefs of Staff
JFC	Joint Forces Command
JFPO	Joint Forces Program Office
JV2010	Joint Vision 2010
JWCA	Joint Warfighting Capabilities Assessment
NETCOM	Network Communications
NMS	National Military Strategy
NSIP	Network Security Improvement Program
OMB	Office of Management and Budget
OSD	Office of the Secretary of Defense
PPBS	Planning, Programming and Budgeting System
PKI	Public Key Infrastructure
POM	Program Objective Memorandum
PSA	Principal Staff Assistant
QDR	Quadrennial Defense Review
RBA	Revolution in Business Affairs
RCAS	Reserve Component Automation Systems
RPSIG	Reserve Personnel Systems Integration Group
RMA	Revolution in Military Affairs
SMI	Security Management Infrastructure
SOW	Statement of Work

SRS	Service Request System
TQM	Total Quality Management
WWW	World Wide Web
Y2K	Year 2000

BIBLIOGRAPHY

A Guide to Planning, Acquiring, and Managing Information Technology Systems. Version 1. Washington, DC: General Services Administration, December 1998.

Andersen, Arthur, Robert Hiebeler, Thomas B. Kelly, and Charles Ketteman. Best Practices: Building Your Business with Customer-Focused Solutions. New York, New York: Simon & Schuster, 1998.

Bass, Len, Paul Clements, and Rick Kazman. Software Architecture in Practice. Reading, Massachusetts: Addison–Wesley Longman, Inc., 1998.

de Czege, Huba Wass and Antulio J. Echevarria II. Toward a Strategy of Positive Ends. Strategic Studies Institute, U.S. Army War College, September 2001.

Department of the Army Enterprise Architecture Guidance Document (AEAGD). Version 1.1, Dec 1998.

Department of the Army, Joint Technical Architecture – Army. Version 5.5, December 1998.

Department of the Army, Personnel Transformation Material Development Campaign Plan, Version 1.5 (Draft). January 2000.

Department of Defense Chief Information Officer. Information Management (IM) Strategic Plan; Information Superiority, Version 2.0. np: October 1999.

Department of Defense. Quadrennial Defense Review Report. September 30, 2001.

English, Larry P. Improving Data Warehouse and Business Information Quality; Methods for Reducing Costs and Increasing Profits. New York, New York: John Wiley & Sons, Inc., 1999.

Forsberg, Kevin, Ph.D.; Hal Mooz, and Howard Cotterman. Visualizing Project Management. New York, New York: John Wiley & Sons, Inc., 1996.

Hallows, Jolyon. Information Systems Project Management: How to Deliver Function and Value in Information Technology Projects. New York, New York: American Management Association, 1998.

Harrington, H. James. Business Process Improvement; The Breakthrough Strategy for Total Quality, Productivity, and Competitiveness. New York, New York: McGraw-Hill, Inc., 1991

Higgins, James M. and Julian Vincze. Strategic Management: Text and Cases. New York, New York: The Dryden Press, 1989.

Keen, Peter G.W. Shaping the Future; Business Design Through Information Technology. Boston, Massachusetts: Harvard Business School Press, 1991.

Lientz, Bennet P. and Kathryn P. Real. Breakthrough Technology Project Management. Second Edition. San Diego, California: Academic Press, 2001.

Linden, Russell M. Seamless Government; A Practical Guide to Re-Engineering in the Public Sector. San Francisco, California: Jossey-Bass Publishers, 1994.

Malhotra, Yogesh. "Knowledge Management for E-Business Performance: Advancing Information Strategy to 'Internet Time." Information Strategy, The Executive's Journal. Vol. 16 (4), Summer 2000.

McLean, Ephraim R. and John V. Soden. Strategic Planning for MIS. New York, New York: John Wiley & Sons, Inc., 1977.

Office of Management and Budget. OMB Circular A-76, Appendix 5: Office of Federal Procurement Policy (OFPP) Policy Letter 92-1, "Inherently Governmental Functions." np: September 1992

`Owens, Dallas D. Jr. AC/RC Integration: Today's Success and Transformation's Challenge. Strategic Studies Institute, U.S. Army War College, October 2001.

Peterson, Brad L. and Diane M. Carco. The Smart Way to Buy Information Technology; How to Maximize Value and Avoid Costly Pitfalls. New York, New York: American Management Association, 1998.

Poe, Vidette; Patricia Klauer, and Stephen Brobst. Building a Data Warehouse. Second Edition. Upper Saddle River, New Jersey: Prentice Hall PTR, 1998.

Rea, Peter, Ph.D. and Harold Kerzner, Ph.D. Strategic Planning a Practical Guide. New York, New York: John Wiley & Sons, Inc., 1997.

Schwartau, Winn. Information Warfare; Cyberterrorism: Protecting Your Personal Security in the Electronic Age. New York, New York: Thunder's Mouth Press, 1996.

Senge, Peter M. The Fifth Discipline: The Art & Practice of the Learning Organization. New York, New York: Currency Doubleday, 1994.

Tenner, Arthur R. and Irving J. DeToro. Process Redesign; The Implementation Guide for Managers. Reading, Massachusetts: Addison Wesley Longman, Inc., 1997.

Toffler, Alvin and Heidi Toffler. War and Anti-War: Survival at the Dawn of the 21st Century. Canada: Little, Brown & Company Limited. 1993.

Turban, Efraim; Ephraim McLean, and James Wetherbe. Information Technology Management: Making Connections for Strategic Advantage. Second Edition. New York, New York: John Wiley & Sons, Inc., 1997.

U.S. Army War College. How the Army Runs: A Senior Leader Reference Handbook. Carlisle Barracks, Pennsylvania. 2001 – 2002.

von Ghyczy, Tiha; Bolko von Oetinger, and Christopher Bassford. Clausewitz on Strategy: Inspiration and Insight from a Master Strategist. New York, New York: John Wiley & Sons, Inc., 2001.